APPENDIX A

Defendant's Motion for *Franks* Hearing

United States v. Curcio, 24-CR-312

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
11512 158th Avenue NE, Redmond, WA 98052, as described more particularly in Attachment A

Case No. MJ24-309

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
11512 158th Avenue NE, Redmond, WA 98052, as described more particularly in Attachment A.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1349, 1343, and 2	wire fraud conspiracy, wire fraud, and aiding and abetting the same.

The application is based on these facts:

✓ See Affidavit of Special Agent Christopher Campbell, FBI, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

_____
Applicant's signature

Christopher Campbell, Special Agent FBI
Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/22/2024

_____
Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, CHRISTOPHER CAMPBELL, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (the "FBI"), assigned to the Major Theft Task Force based in New York City. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the FBI since October 2000. Over the course of my career, I have participated in numerous investigations involving fraud, including fraud schemes involving the use of electronic communications to effect such schemes, and have conducted and participated in surveillance, interviews of witnesses, and the execution of search warrants, including the execution of search warrants involving the seizure of electronically stored information ("ESI"). I have also become familiar with the ways in which individuals engaged in fraud crimes use ESI and electronic communications to facilitate illicit activities. As a law enforcement officer, I have also received training relating to the search and review of electronic devices. I have been personally involved in the investigation of this matter.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at **11512 158th Avenue NE, Redmond, WA 98052**, hereinafter "SUBJECT PREMISES," as more fully described in Attachment A to this Affidavit, for the property and items

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

described in Attachment B to this Affidavit, as well as any digital devices or other electronic storage media located therein.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of cooperating witnesses; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 1349 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and abetting the same) (collectively, the "Subject Offenses") will be found at the SUBJECT PREMISES.

THE INVESTIGATION

5. As set forth in the criminal Indictment (the "Indictment") that was returned by a grand jury in the Southern District of New York on May 20, 2024, which is incorporated herein by reference, ANTHONY CURCIO, a/k/a "Brendan Wooley" ("Target Subject-1" or "CURCIO"), and IOSIF BONDARCHUK, a/k/a "Joe Bondarchuk" ("Target Subject-2" or "BONDARCHUK") (collectively, the "Target Subjects"), from at least in or about 2022 up to and including in or about May 2024, engaged in a fraudulent scheme to defraud buyers and marketplaces to purchase sports and Pokémon trading cards at false and inflated prices by misrepresenting that low-to-mid grade cards had received high-grade ratings from a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

reputable card authentication company ("Company-1"), thereby causing victims to pay more money for the cards than they otherwise would have. In total, the Target Subjects attempted to deprive victims of over $2 million through their sales and attempted sales of trading cards by misrepresenting the grade of numerous trading cards.

6. As is further set forth in the Indictment:

a. Sports and Pokémon trading cards containing the images of professional athletes and Pokémon can have considerable collectible and resale value depending on, among other things, their condition and authenticity. Company-1 is a prominent card authenticator and grader. For a fee, Company-1 verifies a card's authenticity, assesses its condition, and assigns it a numerical grade from one to ten, with one being the lowest grade and ten being the highest grade. The grade assigned is reflective of the card's comparative market value. After grading a card, Company-1 seals the card in a distinctive, tamper-resistant plastic case that encloses the card to preserve its condition and indicates its grade on an affixed label.

b. The card grade assigned by Company-1 significantly impacts the market value of the card. As an example, a 1986 Fleer Michael Jordan #57 card graded as an 8 has an estimated market value of between $6,000 and $7,000. But this same card, when graded as a 10 by Company-1, has had an estimated market value of between approximately $185,000 and $203,000. In short, representations about Company-1's grade of the card go directly to the value of the card itself and the price at which the card can be bought and sold.

c. The Target Subjects sold and attempted to sell sports and Pokémon trading cards through, among other means, an online card marketplace based in Manhattan (the "Manhattan Marketplace"). Through the Manhattan Marketplace, the Target Subjects sold various cards at inflated prices by falsely claiming the cards had been assigned higher ratings by Company-1 than was true.

d. Among the cards that the Target Subjects sold as part of the scheme through the Manhattan Marketplace was a 1986 Fleer Michael Jordan #57 card (the "1986 MJ Card"). In or about May 2022, CURCIO advertised one version of the 1986 MJ Card on the Manhattan Marketplace for sale for the amount of $171,700, as pictured below.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As is depicted above, Target Subject-1 advertised the 1986 MJ Card as having a purported grade of "10" assigned by Company-1. In truth and in fact, Target Subject-1 knew that Company-1 had not assigned this grade to the card. To make it appear that the 1986 MJ Card had received a grade of 10 from Company-1, Target Subject-1 caused the 1986 MJ Card to be displayed in in the distinctive, tamper-resistant plastic case of Company-1 with a labeled rating of 10, when, in reality, the 1986 MJ Card he was offering for sale had received no such rating from Company-1. Through this fraudulent scheme, Target Subject-1 made these misrepresentations to fraudulently inflate the card's value and induce victims to pay more money for the 1986 MJ Card than they otherwise would have paid. To further make it appear that the 1986 MJ Card had received a rating of 10 from Company-1, Target Subject-1

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

caused a purported Company-1 label to be included in the plastic case, along with a fraudulent bar code and certification number.

e. During the fraudulent trading card scheme, when victims demanded refunds and confronted the Target Subjects over the misrepresented, fraudulent cards, including by showing the Target Subjects confirmations from Company-1 that the Target Subjects had misrepresented the grade of the cards, the Target Subjects feigned ignorance and often refunded the victims. Yet, after being put on notice that the cards' grades and labels were fraudulent, the Target Subjects repeatedly attempted to, and did, sell these very same cards to subsequent victims, again with fraudulent labels showing an inflated, grade from Company-1.

f. The Target Subjects sold and attempted to sell fraudulently misrepresented cards using several different methods, including online sales through the Manhattan Marketplace. The Target Subjects completed at least eight fraudulent sales, totaling $225,000 in value, through the Manhattan Marketplace. The Target Subjects repeatedly sent a variety of interstate wires into and out of Manhattan in furtherance of the fraud, including posts on the Manhattan Marketplace's website, messages to website administrators, and messages to individual victims through the website's messaging portal. The Target Subjects also sold and attempted to sell fraudulently misrepresented cards at in-person card shops, auctions, and card shows.

g. The Target Subjects also fraudulently misrepresented the Company-1 grade of Pokémon trading cards to induce victims to pay more money for the cards than they otherwise would have paid. Among the fraudulently misrepresented cards that the Target Subjects sold and attempted to sell are a 1999 Pokémon Venusaur card and a 1999 Pokémon Charizard card, pictured below.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In or about July 2023, as part of a law enforcement undercover purchase of the above fraudulently misrepresented 1999 Pokémon Venusaur card for $10,500—which card Target Subject-2 had previously attempted to sell on an online marketplace—Target Subject-1 mailed the card to the undercover law enforcement purchaser at an address in Manhattan after the undercover purchaser wired the money to a bank account that Target Subject-1 controlled.

7. Based on information provided to me and other law enforcement agents by certain victims of the fraudulent trading card scheme, my discussions with other law enforcement agents, my training and experience, and my participation in this investigation, I have learned that Target Subject-1 repeatedly provided the SUBJECT PREMISES as his shipping address to victims. Specifically, when victims learned that the trading cards were fraudulent and demanded refunds and/or otherwise confronted Target Subject-1 about the fraudulent trading cards, among other things, Target Subject-1 asked the victims to return the fraudulent trading cards to him by mailing the cards to the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUBJECT PREMISES. A victim returned a fraudulent card to Target Subject-1 at the TARGET PREMISES as recently as September 2023.

8. Based on purchase records produced to law enforcement pursuant to a grand jury subpoena served upon an online marketplace, my discussions with other law enforcement agents, my training and experience, and my participation in this investigation, I have learned that, during the fraudulent trading card scheme, Target Subject-1 ordered various items needed to create forged card cases and labels to be delivered to his listed residence, the SUBJECT PREMISES. Specifically, between in or about June 2022 and in or about February 2024, Target Subject-1 purchased various card grading cases, thermal transfer barcode labels, a magnifier loupe optical glass, a handheld inkjet printer, a lock-cutting kit, an electric grinding pen, an abrasive buffer and polishing wheel, an abrasive and bristle brushes, and drill bits designed for engraving. The most recent purchase, in February 2024, was for drill bits designed for engraving.

9. Based on flight records obtained by law enforcement pursuant to a database search, my discussions with other law enforcement agents, my training and experience, and my participation in this investigation, I have learned that Target Subject-1 attended a card show as recently as April 2024, in New Jersey, where he was identified and removed from the show for having fraudulent cards. Target Subject-1 flew directly from Seattle to Newark, New Jersey, to attend this card show.

10. Based on records produced to law enforcement pursuant to grand jury subpoenas served upon phone companies and financial institutions, my discussions with other law enforcement agents, my training and experience, and my participation in this investigation, I have learned that the SUBJECT PREMISES are listed as Target Subject-1's address on Target Subject-1's driver's license and bank records. Target Subject-1 lives with his wife and two children at the SUBJECT PREMISES. Surveillance was conducted on the SUBJECT PREMISES on multiple days in May 2024. As recently as May 21, 2024, the Target Subject-1 was viewed at the SUBJECT PREMISES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

11. As is described above and in the Indictment, it appears that Target Subject-1 used the SUBJECT PREMISES to further the fraudulent trading card scheme. Based on my training and experience and my participation in this investigation, including my review of Target Subject-1's communications with victims, there is probable cause to believe that the SUBJECT PREMISES will include, among other things, fraudulent trading cards and certain tools and equipment needed to create forged card cases and labels in connection with the commission of the Subject Offenses.

12. Based on my training and experience, I know that individuals who engage in the Subject Offenses routinely store the proceeds of their crimes in their residences. In addition, I know that within their residences, individuals who engage in the Subject Offenses often store the proceeds of their crimes in safes, key-lock strong boxes, suitcases, locked cabinets, and other types of locked or closed containers. I therefore seek authorization to open any closed items and containers or to seize any such closed items and containers so that they may be opened if tools or other implements are required.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

13. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices[1]

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

such as computer hard drives or other electronic storage media.[2] Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

14. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the Subject Offenses will be stored on those digital devices or other electronic storage media.

15. Based on information provided to me and other law enforcement agents by certain victims of the fraudulent trading card scheme, my discussions with other law enforcement agents, my training and experience, and my participation in this investigation, I have learned that Target Subject-1 uses electronic devices to communicate with victims. Specifically, based on the foregoing, I know that Target Subject-1 communicated with victims via emails, phone calls, and text messages.

16. Based on my training and experience, I know that individuals who engage in the Subject Offenses commonly use cellphones and other electronic devices to communicate in furtherance of their criminal scheme, including by using email, text messages, messaging applications, and voice calls to communicate with any co-conspirators or aiders or abettors and victims. Indeed, as stated above, during the course of this investigation, I have reviewed electronic communications of Target Subject-1 with certain victims of the Subject Offenses that occurred by email and text message. Based on my training and experience, I know that individuals who engage in fraud schemes

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

often store data on their cellphones related to their illegal activity, which can include logs of online "chats" with co-conspirators and victims; email and other electronic correspondence with co-conspirators and victims; contact information of co-conspirators and victims, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; and records of the disposition of criminal proceeds, among other things.

17. Based on my training, experience, and research, I know that while cellphones and smartphones both have voice call and messaging capabilities, smartphones also have capabilities that allow them to serve as a wireless telephone, digital camera, internet-capable device, and GPS navigation device, among other things. Accordingly, cellphones and smartphones often contain information such as contact lists (including phone numbers) and text and photo messages. Smartphones also often contain photos, internet-browsing history, GPS information, and messaging content.

18. Based on the foregoing, there is probable cause to believe that evidence, fruits and/or instrumentalities of the Subject Offenses exists and will be found on digital device or other electronic storage media at the SUBJECT PREMISES, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the SUBJECT PREMISES because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[1] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running

[1] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

20. There is probable cause to believe that the SUBJECT PREMISES contains electronic, digital devices that contain evidence, fruits and instrumentalities of the Subject Offenses. In particular, based on information provided to me and other law enforcement agents by certain victims of the fraudulent trading card scheme, my discussions with other law enforcement agents, my training and experience, and my participation in this investigation, I have learned that Target Subject-1 uses electronic devices to communicate with victims of the Subject Offenses. Specifically, based on the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

foregoing, I know that Target Subject-1 communicated with victims via emails, phone calls, and text messages.

a. In particular, there is probable cause to believe that electronic devices in the SUBJECT PREMISES contain email communications concerning the Subject Offenses. For instance, Target Subject-1's laptop and smartphone are likely to contain emails about the exchange of trading cards for money or other trading cards given that, as recently as April 2024, a victim exchanged such emails with Target Subject-1.

b. Moreover, there is probable cause to believe that electronic devices in the SUBJECT PREMISES contain logs of phone calls relating to the Subject Offenses. For instance, Target Subject-1's cellphone is likely to contain such evidence because, in connection with this investigation, law enforcement has obtained an audio recording of a call between Target Subject-1 and a particular victim concerning the Subject Offenses.

c. Finally, there is probable cause to believe that cellphones and smartphones in the SUBJECT PREMISES contain text messages concerning the Subject Offenses. For instance, Target Subject-1's cellphones are likely to contain text messages concerning the return and refund of certain fraudulent trading cards because, in connection with this investigation, law enforcement has obtained text messages with certain victims that show Target Subject-1 directing the victims to return the fraudulent trading cards to him by mailing the cards to the SUBJECT PREMISES.

21. Based on my training and experience, I know that individuals who engage in the Subject Offenses commonly use cellphones and other electronic devices to communicate in furtherance of their criminal scheme, including by using email, text messages, messaging applications, and voice calls to communicate with any co-conspirators or aiders or abettors and victims. Indeed, as stated above, during the course of this investigation, I have reviewed electronic communications of Target Subject-1 with certain victims of the Subject Offenses that occurred by email and text message. Based on my training and experience, I know that individuals who engage in fraud schemes often store data on their cellphones related to their illegal activity, which can include logs of online "chats" with co-conspirators and victims; email and other electronic correspondence with co-conspirators and victims; contact information of co-conspirators

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and victims, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; and records of the disposition of criminal proceeds, among other things.

22. Based on my training, experience, and research, I know that while cellphones and smartphones both have voice call and messaging capabilities, smartphones also have capabilities that allow them to serve as a wireless telephone, digital camera, internet-capable device, and GPS navigation device, among other things. Accordingly, cellphones and smartphones often contain information such as contact lists (including phone numbers) and text and photo messages. Smartphones also often contain photos, internet-browsing history, GPS information, and messaging content.

23. Because of the nature of the evidence that I am attempting to obtain and the nature of the investigation, I have not made any prior efforts to obtain the evidence based on the consent of any party who may have authority to consent. I believe, based upon the nature of the investigation and the information I have received, that if Target Subject-1 becomes aware of the investigation in advance of the execution of a search warrant, he may attempt to destroy any potential evidence, whether digital or non-digital, thereby hindering law enforcement agents from the furtherance of the criminal investigation.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

24. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

REQUEST FOR AUTHORITY TO OBTAIN PHYSICAL BIOMETRIC CHARACTERISTICS

25. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face, iris, or retina. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. While not as prolific on digital devices as fingerprint and facial-recognition features, both iris and retina scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device, and may not be the only individual whose physical characteristics are among those that will unlock the device via biometric features. Furthermore, while physical proximity is an important factor in determining who is the user of a device, it is only one among many other factors that may exist.

i. Due to the foregoing, I request that if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and if law enforcement reasonably suspects ANTHONY CURCIO is a user of the device, then – for the purpose of attempting to unlock the device in order to search the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contents as authorized by this warrant – law enforcement personnel shall be authorized to:(1) press or swipe the fingers (including thumbs) of CURCIO to the fingerprint scanner of the device; and/or (2) hold the device in front of the face and open eyes of CURCIO and activate the facial, iris, or retina recognition feature.

j. In pressing or swiping an individual's thumb or finger onto a device and in holding a device in front of an individual's face and open eyes, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

SEARCH TECHNIQUES

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

27. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless reasonably suspect that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

28. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

A. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit. [3]

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A

[3] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

B. Searching the Forensic Images.

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

CONCLUSION

29. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1349 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and abetting the same) are located at the SUBJECT PREMISES, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found at the SUBJECT PREMISES. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES, as well as any digital devices and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic storage media located therein, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

30. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

CHRISTOPHER CAMPBELL
Special Agent
Federal Bureau of Investigation

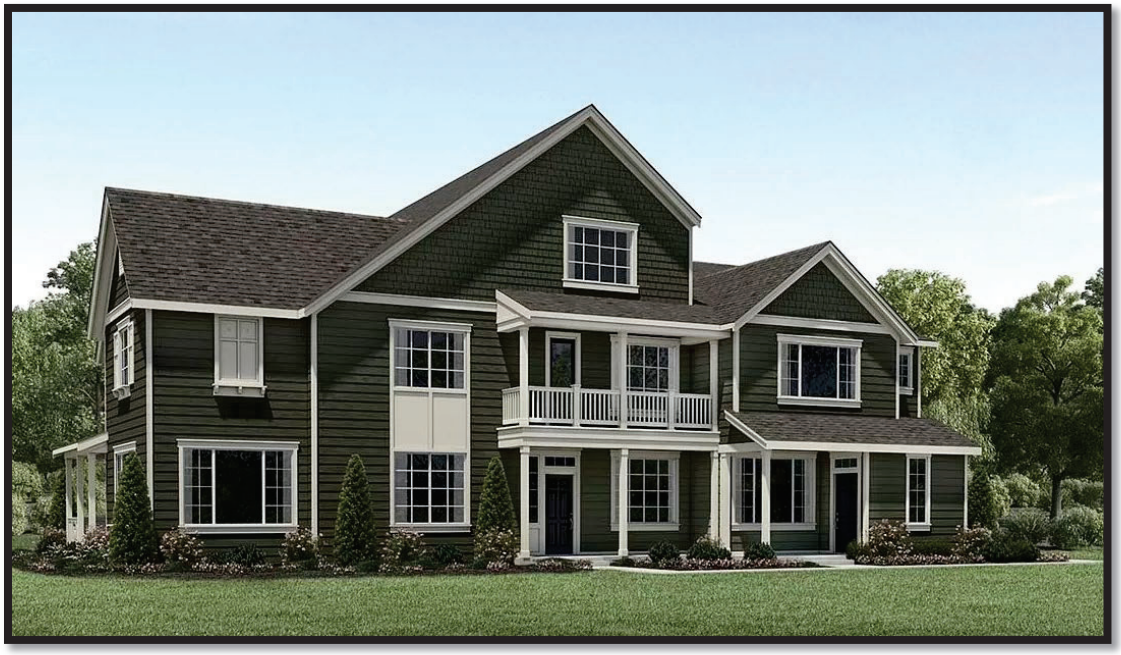
The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on the 22nd day of May, 2024.

MICHELLE L. PETERSON
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

The property to be searched is 11512 158th Ave NE, Redmond, WA 98052, further described as multi-story, single-family home, and any digital devices or other electronic storage media found therein. The street view and side view of the SUBJECT PREMISES are depicted in the following photographs:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 1349 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and abetting the same) (collectively, the "Subject Offenses") involving Target Subject-1, ANTHONY CURCIO:

1. Evidence concerning occupancy or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

2. Trading cards and Pokémon cards located within the SUBJECT PREMISES;

3. Any tools, materials, and/or equipment that may be used to create forged card cases and labels;

4. For the time period of January 1, 2022 to the present, evidence relating to the Target Subjects communicating with victims, with each other, and with co-conspirators;

5. For the period of January 1, 2022 to the present, evidence of communications constituting or discussing or regarding the commission of the Subject Offenses;

6. Evidence concerning the identities and locations of co-conspirators and victims;

7. Evidence of criminal conduct, including communications reflecting an agreement between the Target Subjects and other co-conspirators to engage in the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

scheme to defraud customers who purchased cards from the Target Subjects and their co-conspirators;

8. Proceeds of the commission of the Subject Offenses, including any bulk cash contained within the SUBJECT PREMISES;

9. Evidence of the use of aliases by the Target Subjects, including documents reflecting false names;

10. Evidence relating to state of mind, including communications relating to the Target Subjects' understanding that certain representations being made to individuals purchasing cards from them were or must have been false;

11. For the time period of January 1, 2022 to the present, evidence of the receipt, transfer, disposition or location of funds derived from the commission of the Subject Offenses;

12. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

13. Evidence of user attribution showing who used or owned an electronic device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

14. Any items or records needed to access the data stored on any seized or copied electronic devices or storage media, including but not limited to any encryption devices, or records of login credentials, passwords, private encryption keys, or similar information;

15. Any items or records that may facilitate a forensic examination of electronic devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied electronic devices or storage media;

16. Location data, including but not limited to geolocation reporting and location history data and metadata associated with other files that would place the Target Subjects and any co-conspirators and/or aiders and abettors, as well as the devices they used, in specific places at specific times, and would indicate the use of their devices during those times;

17. Safes, key-lock strong boxes, suitcases, locked cabinets, and other types of locked or closed containers used to secrete and store currency, electronic devices, identification documents, books, records, financial instruments, and other and other

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

items within the categories described herein. Law enforcement agents executing this warrant are specifically authorized to open any such locked safes or containers including, where necessary, by using reasonable force. Law enforcement agents shall not seize locked safes or containers that do not contain evidence or fruits of the Subject Offenses, unless the safes or containers cannot be opened using reasonable force at the SUBJECT PREMISES. Any locked safe or container that can only be opened away from the SUBJECT PREMISES shall be returned if a later search shows that it does not contain evidence or fruits of the Subject Offenses;

18. Evidence concerning the location of other evidence of the Subject Offenses, including but not limited to information concerning addresses of other premises potentially containing relevant evidence, financial accounts where criminal proceeds may be stored, and communications reflecting registration of online accounts potentially containing relevant evidence;

19. Digital devices[2] or other electronic storage media[3] that law enforcement reasonably suspects belong to Target Subject-1, ANTHONY CURCIO, containing any of the records or information described above or used as a means to commit the violations described above, including to generate, store, or transmit records in furtherance of the violations.

20. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, that may contain things otherwise called for by this warrant, or whose seizure is otherwise authorized by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms

---

[2] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[3] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

h. passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

i. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

j. applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

k. contextual information necessary to understand the evidence described in this attachment.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

During the execution of the search of the SUBJECT PREMISES described in Attachment A, if law enforcement encounters a smartphone or other electronic device equipped with a biometric-unlock feature, and if law enforcement reasonably suspects ANTHONY CURCIO is a user of the device, then – for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant – law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of CURCIO to the fingerprint scanner of the device; and/or (2) hold the device in front of the face and open the eyes of CURCIO and activate the facial, iris, or retina recognition feature.

In pressing or swiping an individual's thumb or finger onto a device and in holding a device in front of an individual's face and open eyes, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

11512 158th Avenue NE, Redmond, WA 98052, as described more particularly in Attachment A

Case No. MJ24-309

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Washington *(identify the person or describe the property to be searched and give its location)*:

11512 158th Avenue NE, Redmond, WA 98052, , as described more fully in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before June 4, 2024 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Any MJ of this District .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 5/22/24, ~~3:00 pm~~ 1400

Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge
Printed name and title

2024R00633

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

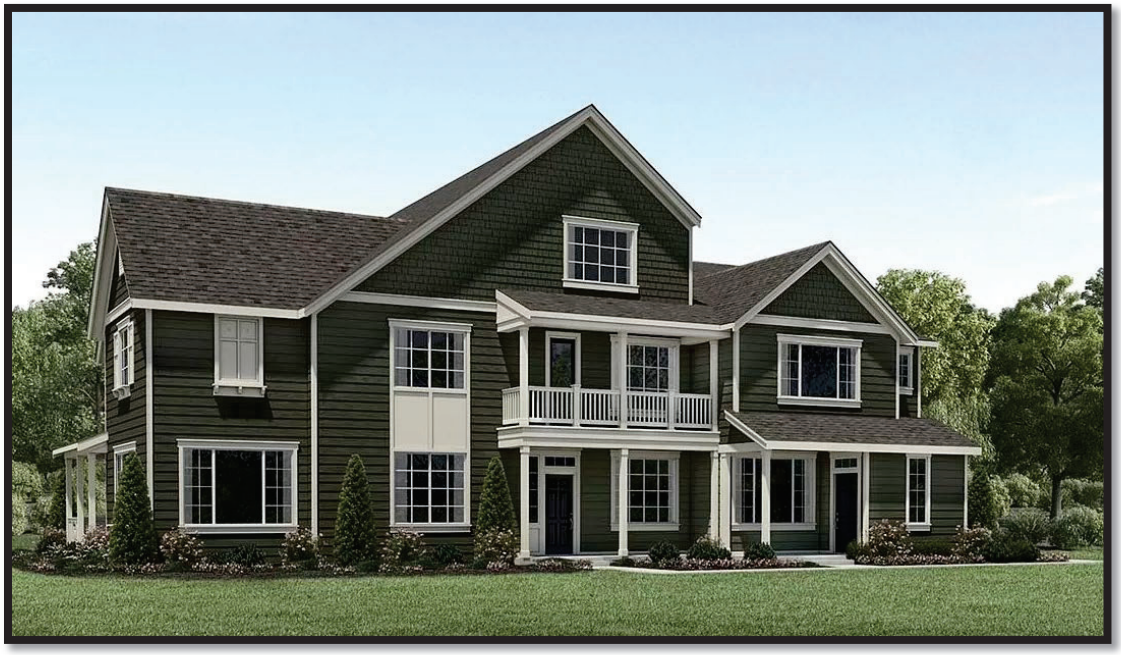
_____
Executing officer's signature

_____
Printed name and title

2024R00633

ATTACHMENT A

The property to be searched is 11512 158th Ave NE, Redmond, WA 98052, further described as multi-story, single-family home, and any digital devices or other electronic storage media found therein. The street view and side view of the SUBJECT PREMISES are depicted in the following photographs:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 1349 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and abetting the same) (collectively, the "Subject Offenses") involving Target Subject-1, ANTHONY CURCIO:

1. Evidence concerning occupancy or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

2. Trading cards and Pokémon cards located within the SUBJECT PREMISES;

3. Any tools, materials, and/or equipment that may be used to create forged card cases and labels;

4. For the time period of January 1, 2022 to the present, evidence relating to the Target Subjects communicating with victims, with each other, and with co-conspirators;

5. For the period of January 1, 2022 to the present, evidence of communications constituting or discussing or regarding the commission of the Subject Offenses;

6. Evidence concerning the identities and locations of co-conspirators and victims;

7. Evidence of criminal conduct, including communications reflecting an agreement between the Target Subjects and other co-conspirators to engage in the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

scheme to defraud customers who purchased cards from the Target Subjects and their co-conspirators;

8. Proceeds of the commission of the Subject Offenses, including any bulk cash contained within the SUBJECT PREMISES;

9. Evidence of the use of aliases by the Target Subjects, including documents reflecting false names;

10. Evidence relating to state of mind, including communications relating to the Target Subjects' understanding that certain representations being made to individuals purchasing cards from them were or must have been false;

11. For the time period of January 1, 2022 to the present, evidence of the receipt, transfer, disposition or location of funds derived from the commission of the Subject Offenses;

12. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

13. Evidence of user attribution showing who used or owned an electronic device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

14. Any items or records needed to access the data stored on any seized or copied electronic devices or storage media, including but not limited to any encryption devices, or records of login credentials, passwords, private encryption keys, or similar information;

15. Any items or records that may facilitate a forensic examination of electronic devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied electronic devices or storage media;

16. Location data, including but not limited to geolocation reporting and location history data and metadata associated with other files that would place the Target Subjects and any co-conspirators and/or aiders and abettors, as well as the devices they used, in specific places at specific times, and would indicate the use of their devices during those times;

17. Safes, key-lock strong boxes, suitcases, locked cabinets, and other types of locked or closed containers used to secrete and store currency, electronic devices, identification documents, books, records, financial instruments, and other and other

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

items within the categories described herein. Law enforcement agents executing this warrant are specifically authorized to open any such locked safes or containers including, where necessary, by using reasonable force. Law enforcement agents shall not seize locked safes or containers that do not contain evidence or fruits of the Subject Offenses, unless the safes or containers cannot be opened using reasonable force at the SUBJECT PREMISES. Any locked safe or container that can only be opened away from the SUBJECT PREMISES shall be returned if a later search shows that it does not contain evidence or fruits of the Subject Offenses;

18. Evidence concerning the location of other evidence of the Subject Offenses, including but not limited to information concerning addresses of other premises potentially containing relevant evidence, financial accounts where criminal proceeds may be stored, and communications reflecting registration of online accounts potentially containing relevant evidence;

19. Digital devices[2] or other electronic storage media[3] that law enforcement reasonably suspects belong to Target Subject-1, ANTHONY CURCIO, containing any of the records or information described above or used as a means to commit the violations described above, including to generate, store, or transmit records in furtherance of the violations.

20. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, that may contain things otherwise called for by this warrant, or whose seizure is otherwise authorized by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms

---

[2] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[3] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

h. passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

i. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

j. applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

k. contextual information necessary to understand the evidence described in this attachment.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

During the execution of the search of the SUBJECT PREMISES described in Attachment A, if law enforcement encounters a smartphone or other electronic device equipped with a biometric-unlock feature, and if law enforcement reasonably suspects ANTHONY CURCIO is a user of the device, then – for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant – law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of CURCIO to the fingerprint scanner of the device; and/or (2) hold the device in front of the face and open the eyes of CURCIO and activate the facial, iris, or retina recognition feature.

In pressing or swiping an individual's thumb or finger onto a device and in holding a device in front of an individual's face and open eyes, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970